„Ante Portas – Security Studies”
2024, No. 21
DOI: 10.33674/1202420

Victoria BEVZIUC[1]
Moldova
Svetlana CEBOTARI[2]
Moldova

CYBER ATTACKS – RUSSIAN FEDERATION'S MECHANISM OF INFLUENCE IN UKRAINE

Abstract: *Currently, the international community is facing a hybrid conflict in Ukraine, where traditional and cyber weapons are being used at the same time. The big surprise of the Russian invasion was the apparent absence of a major cyber war. In addition to physical attacks on Ukraine, Moscow has resorted to launching cyber-attacks. For years, cyberspace has been considered a space where warfare can take place beyond space cyberspace has been considered a space where warfare can take place beyond land, water, or airspace. Since then, a multitude of cyber-attacks on Ukrainian infrastructure and its allies have been observed, of different types and with different objectives. This article highlights the main aspects of the cyber-attacks launched by the Russian Federation on Ukraine. Moreover, this article shows how the Ukrainian war may change the traditional parameters of international conflicts.*

Keywords: *threat, cyber security, cyber war, cyber attack, Russia, Ukraine, hackers*

Introduction

The presence of a high-intensity war on the European territory has marked the use of cyberspace as a battlefield between the Russian Federation and the West, including the Russian Federation and Ukraine. The cyber attacks have

[1] Victoria Bevziuc, PhD, Moldova State University, ORCID: 0000-0001-9189-641X, email: victoriabevziuc@yahoo.ro

[2] Svetlana Cebotari, PhD, DSc, Moldova State University, ORCID: 0000-0001-9073-104X, email: svetlana.cebotari11@gmail.com

now become an essential element of conflicts in the modern era, as demonstrated by the actions of both state and non-state actors in the cyber domain during the Russo-Ukrainian war[3].

According to the military theories, alongside the sea, air, land, and space domains, the cyber space is designated as the fifth domain of warfare. Today, we are witnessing a significant expansion of this fifth domain, with a multitude of cyber attacks being observed targeting the Ukrainian infrastructure and its allies, of various types and with different objectives.

For years, cyberspace has been considered a realm where warfare can occur beyond land, sea, or space domains, with a multitude of cyber attacks observed against Ukrainian infrastructure and its allies, of various types and with different objectives. Thus, Russia's invasion of Ukraine has altered both the real and virtual worlds. However, this moment is not a new one, as the current war stems from the prolonged Russo-Ukrainian conflict that began in 2014, characterized by Russian cyber attacks on critical Ukrainian infrastructure[4].

Conceptual distinctions between the terms "cyber warfare" and "cyber attack"

In today's increasingly digital world, cyber warfare is no longer a futuristic concept; it represents a real and significant threat to the national security and the interests of a nation[5]. Although some researchers consider cyber warfare equivalent to cyber attacks, there is a significant difference between these two terms. According on the theses put forth in 2009 by Martin Libicki, an expert on cyber warfare issues, in a report he wrote for the US Air Force, he presented a definition of "cyber warfare". Libicki considers cyber warfare as a directed and individualized war, not involving "real" or physical war, but rather a virtual one. Libicki mentions that "cyber warfare will play an important role in the future." Additionally, the author considers cyber warfare as possibly part of special warfare and focused on the use of so-called "soft power"[6]. For Libicki,

[3] *Dimensiunea cibernetică a conflictului Rusia – Ucraina – Deslușirea primei etape*, <https://dnsc.ro/citeste/dimensiunea-cibernetica-conflictului-rusia-ucraina-deslusirea-primei-etape> (12.09.2024).

[4] A. Gavrila, *La gran ciberguerra de Ucrania que no ocurrió*, <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO99_2022_ADAGAV_Ucrania.pdf> (12.09.2024).

[5] J. Mackay, *Cyber warfare: ¿Qué es la guerra cibernética?*, <https://www.metacompliance.com/es/blog/security-awareness-training/what-is-cyber-warfare> (20.04.2024).

[6] D. Trifunović, Z. Bjelica, *Cyber war – trends and technologies*, <https://www.researchgate.net/publication/349942064_Cyber_War_-_Trends_and_Technologies> (19.94.2024).

the cyber warfare is the systematic use of information, messages, etc., to attack information systems[7].

Analyzing the specifics of warfare, R. Guedes considers a "cyber warfare" as a form of conflict that takes place in the virtual space, where weapons are electronic devices, and the main objective is the control or destruction of information systems, communication networks, and critical infrastructure. This type of warfare can be conducted by governments, terrorist organizations, hacker groups, or individuals and can have devastating consequences for society, from economic damage to national security risks. The cyber warfare presents unique challenges compared to other forms of conflict due to its transnational and anonymous nature[8]. Additionally, a cyber warfare is used to destabilize a country by attacking critical infrastructure, such as national power grids, financial markets, or military databases. The damage resulting from such a large-scale attack could be devastating[9].

The cyber warfare exists in both the military and information domains, referring to the conduct of military operations based on informational principles. This involves disrupting or destroying information and communication systems. It also entails attempting to learn everything about the adversary while simultaneously reducing their attempts to learn too much about you. The cyber warfare is similar to traditional armed conflict, with differences lying in the environment of engagement - virtual - and the means through which it is conducted - networks and ICT (Information and Communication Technology) tools. Like other forms of warfare, the purpose of cyber warfare is to achieve certain interests - political, territorial, economic, or ethnic - by affecting the adversary's decision-making capacity, both politically and militarily, through operations in computer networks[10].

Three types of operations in computer networks can be distinguished: attacks - operations designed to disrupt, impede, degrade, or destroy information residing in computers or networks or even enemy computers and networks; espionage - gathering data and information from the adversary's computers through ICT means; defense - taking all necessary measures to protect one's own ICT means and infrastructure against the opponent's attacks

[7] M. C. Libicki, *Cyberwar as a Confidence Game*, <https://www.jstor.org/stable/26270514?seq=8> (19.09.2024).

[8] R. Guedes, *Guerra Cibernética: Tipos, Armas, Objetivos y Ejemplos de Guerra Tecnológica*, <https://ciberprisma.org/2023/05/10/guerra-cibernetica-tipos-armas-objetivos-y-ejemplos-de-guerra-tecnologica/> (19.09.2024).

[9] *Cyber warfare: ¿Qué es la guerra cibernética?*, <https://www.metacompliance.com/es/cyber-security-terminology/cyber-warfare> (19.09.2024).

[10] D. Trifunović, Z. Bjelica, *Cyber war – trends and technologies*, https://www.researchgate.net/publication/349942064_Cyber_War_-_Trends_and_Technologies> (20.09.2024).

and espionage. Thus, at a conceptual level, cyber attacks cover only a small portion of the total operations in computer networks[11].

Richard A. Clarke defines cyber warfare as actions sponsored by a nation-state to penetrate the networks or computers of other nations with the aim of causing damage or sabotage[12].

As in conventional warfare, the primary objective of cyber warfare is to weaken the country by undermining social cohesion, political stability, and military and industrial capacity. Although the boundaries between cyber warfare, cybercrime, and cyber terrorism may be blurred, cyber warfare is not primarily motivated by economic gain and is committed by agents affiliated with a country. The cyber warfare can include attacks against[13]:

- civil infrastructures, such as power grids or traffic management systems;
- financial entities, such as banks and credit unions;
- military installations, contractors, and other national security institutions;
- private citizens of the affected country.

Unlike the term "cyber warfare," the term "cyber attack" refers to any intentional effort to steal, expose, modify, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system, or digital device[14]. Referring back to J. Mackay's thesis, a cyber attack represents an operation conducted in computer networks aimed at disrupting, impeding, degrading, or destroying information present in enemy computers and networks[15]. The cyber attacks or the deliberate paralysis or destruction of enemy networks represent one of the numerous tools within military missions. A cyber attack is an elaborate hacking attack meant to undermine the computer security system. This type of attack can be considered a modern form of aggression, given the severity of its consequences comparable to an armed act[16].

A cyber attack represents any intentional effort to steal, expose, modify, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system, or digital device. In today's connected digital

[11] J. Mackay, *Cyber warfare: ¿Qué es la guerra cibernética?*, <https://www.metacompliance.com/es/blog/security-awareness-training/what-is-cyber-warfare> (19.09.2024).

[12] <https://www.cisco.com/c/dam/global/es_mx/products/pdfs/58-60-bridge.pdf> (19.09.2024).

[13] O. Buxton, *Ciberguerra: tipos, ejemplos y cómo protegerse*, <https://www.avast.com/es-es/c-cyber-warfare> (19.09.2024).

[14] *¿Qué es un ataque cibernético?*, <https://www.ibm.com/mx-es/topics/cyber-attack> (19.09.2024)

[15] James Mackay, *op. cit.*

[16] D. Arman, *Atacul cibernetic-o nouă formă de agresiune în dreptul internațional*, <https://ibn.idsi.md/sites/default/files/imag_file/28-31_23.pdf> (19.09.2024).

landscape, cybercriminals use sophisticated tools to launch cyber attacks. The cyber attacks come in various forms through computer networks and systems[17]:

- Malware or malicious software disguises itself as an email attachment or trusted program (e.g., encrypted document or file folder) to exploit viruses and allow hackers to penetrate a computer network. This type of cyber attack often disrupts an entire IT network. Some examples of malware include Trojans, spyware, worms, viruses, and adware;
- Distributed Denial of Service (DDoS) attacks involve multiple compromised computer systems attacked by hackers targeting a website or network and denying user activity on that website or network. For example, hundreds of pop-up windows, ads, and even a crashing website can contribute to a DDoS attack on a compromised server;
- Phishing is the act of sending fraudulent email messages on behalf of reputable companies. Hackers use phishing to gain access to data in a personal or corporate network;
- A SQL injection attack is where a cybercriminal exploits software, taking advantage of applications (e.g., LinkedIn, Target) to steal, delete, or gain control over data;
- Cross-Site Scripting (XSS) is the attack where a cybercriminal sends a link to a website that launches spam or is "script-injected," and it opens, delivering personal information to that cybercriminal;
- Botnet attacks involve multiple computers, typically from a private network, infected with viruses and other forms of malicious software, such as pop-up messages or spam;
- Ransomware is a type of malicious software or malware that threatens a victim by destroying or blocking access to critical data or systems until a ransom is paid.

Thus, if cyber warfare is a form of conflict conducted in the virtual space, carried out through electronic devices to pursue political, territorial, economic, or ethnic interests, as well as to impose the control or destruction of information systems by affecting communications networks and critical infrastructure of the adversary through operations, cyber attack represents an operation, a mechanism through which cyber warfare is carried out.

The impact of cyber attacks by the Russian Federation on Ukraine

There is a need to analyze cyber attacks during the conflict, for a better understanding of the impact of the Russo-Ukrainian war on security, especially

[17] *¿Qué es un ataque cibernético?*, <https://www.ibm.com/mx-es/topics/cyber-attack> (20.09.2024).

on cybersecurity, starting from the day of invasion (February 24, 2022)[18]. Thus, over two years since the emergence of the war, conditioned by the unjustified invasion of Ukraine by the Russian Federation on February 24, 2022, one of the threats added to humanitarian, political, or economic security is cybersecurity. It is noteworthy that the first signs of Russia's invasion into Ukraine appeared in cyberspace[19], looking back at the events in Ukraine. Russia initiated its war against Ukraine on February 24, 2022, but Russian cyber attacks against Ukraine have persisted since Russia's illegal annexation of Crimea in 2014, intensifying even before the 2022 invasion.

The evolution of cyber attacks is determined by the launch of the Russian military operation against Ukraine. Many researchers even agree that the first offensive in the Russo-Ukrainian war was cyber in nature and began at least a month before the emergence of physical warfare. Therefore, we can mention that as early as January 2022, the Ukrainian government faced DDoS (Distributed Denial of Service) cyber attacks launched by the Russian Federation against 70 government websites. Some of these attacks issued a warning to Ukrainians to "prepare for the worst." Thus, analyzing the war in Ukraine, it is noteworthy that Russian intervention in Ukraine was accompanied by large-scale operations not only in land and space domains but also in cyberspace even before February 24, 2022. Additionally, several security experts assert that they observed attacks against Ukrainian information systems[20] just hours before the bombardments launched by the Russian Federation against Ukraine. A series of DDoS attacks were launched against the websites of banks and Ukrainian government departments, rendering them inaccessible[21] with Kiev officially recording over 2,000 cyber attacks from Moscow[22].

Starting from December 12, 2022, cyber attacks by Russian hackers disrupted services provided by Ukraine's largest telecommunications operator

[18] *Dimensiunea cibernetică a conflictului Rusia – Ucraina - Deslușirea primei etape*, <https://dnsc.ro/citeste/dimensiunea-cibernetica-conflictului-rusia-ucraina-deslusirea-primei-etape> (12.09.2024).

[19] *Rusia coordina ciberataques en Ucrania, según Microsoft*, <https://www.dw.com/es/rusia-coordina-ataques-cibern%C3%A9ticos-y-militares-en-ucrania-seg%C3%BAn-microsoft/a-61615216> (12.09.2024).

[20] C. Blanc-Rolin, *Conflit Russie-Ukraine: la guerre est aussi cyber*, <https://www.dsih.fr/article/4608/conflit-russie-ukraine-la-guerre-est-aussi-cyber.html> (12.09.2024).

[21] *5 amenințări asupra securității cibernetice a statelor europene în contextul războiului ruso-ucrainean*, <https://bit-sentinel.com/ro/5-amenintari-asupra-securitatii-cibernetice-a-statelor-europene-in-contextul-razboiului-ruso-ucrainean/> (12.09.2024).

[22] J. C. de Santos, *Ucrania | La realidad ha dejado a la guerra cibernética en un segundo plano*, <https://es.euronews.com/2023/02/22/ucrania-la-realidad-ha-dejado-a-la-guerra-cibernetica-en-un-segundo-plano> (12.09.2024).

for approximately 24 million users for several days. According to statements from Illia Vitiuk, the head of the cybersecurity department at the Security Service of Ukraine (SBU), the cyber attacks caused "disastrous" damage, wiping out "almost everything," including thousands of virtual servers and PCs. Vitiuk describes this attack as the first example of a destructive cyber attack that "completely destroyed the core of a telecommunications operator" such as Kyivstar. Kyivstar is the largest of the three major telecommunications operators in Ukraine, and there are approximately 1.1 million Ukrainians living in towns and small villages where there are no other providers.

Additionally, according to SBU estimates, hackers stole personal information to track phone locations and intercept SMS messages, as well as stole Telegram accounts. The cyber attack on Kyivstar hastened Ukrainian citizens to obtain other SIM cards, creating long queues. ATMs using Kyivstar SIM cards for internet stopped working, and the air raid siren - used during missile and drone attacks - did not function properly in some regions. However, according to I. Vitiuk's statements, the attack did not have a significant impact on the Ukrainian army, which did not rely on telecommunications operators and used other "algorithms and protocols".

The cyber attack on Kyivstar was carried out by Sandworm, a Russian military intelligence cyber warfare unit that infiltrated a Ukrainian telecommunications operator. Additionally, cyber attacks by Sandworm were supported by the affiliated group called Solntsepyok, also responsible for the attack. Similarly, Sandworm was behind the cyber attacks on Ukraine's power grid in 2017 and the NotPetya malware operation[23].

For the conduct of a cyber war, which has both defensive and offensive characteristics, multiple methods of operation are used, as highlighted by Yannick Chatelain: "Both through the use of cyber propaganda and through DDoS attacks that aim to saturate a server or render a website unavailable, or even through data destruction by malicious software"[24]. The Russian invasion of Ukraine has led to the emergence of the first cyber war in history. The Russo-Ukrainian war is not only taking place on the ground; it also extends into cyberspace. Thus, according to research conducted by Yannick Chatelain, a professor at the Grenoble School of Management and a specialist in digital technology, we are currently witnessing the confrontation with the first cyber war of international dimensions[25].

[23] T. Balmforth, *Exclusive: Russian hackers were inside Ukraine telecoms giant for months*, <https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/> (12.09.2024).

[24] *Guerre en Ukraine: Pourquoi parle-t-on d'une cyberguerre*?, <https://guardia.school/le-lab/guerre-en-ukraine-pourquoi-parle-t-on-dune-cyberguerre.html> (12.09.2024).

[25] *Ibidem*.

We are currently witnessing the unfolding of a "cyber war", analyzing Russia's attacks on Ukraine, This is also the opinion of Major General Jürgen Setzer of the Cyber and Information Domain Command (KdoCIR) of the Bundeswehr when referring to Russia's attacks in the war against Ukraine. According to Setzer's opinion, governments' activities can be paralyzed or weakened through other means such as disinformation, fake news, and cyber attacks on vital infrastructure such as power grids, roads, railways, or hospitals. In this way, the objectives set by adversaries could be achieved "without resorting to weapons." However, the real dimension of the virtual war in Ukraine is unclear for a simple reason: "it is very difficult to establish the limits, the boundaries of cyberspace," Setzer explains. In other words, the virtual attacks are usually invisible at first, but their consequences can be immediate. On the other hand, conventional warfare maneuvers can be seen on television channels or social media networks.

There is no doubt that the war in Ukraine is being fought on two levels for cyber issues expert Regine Grienberger from the German Ministry of Foreign Affairs. Grienberger distinguishes between two types of combatants: conventional troops on the battlefield and invisible virtual warriors - "cyber mercenaries," who operate from completely different states and continue to participate in combat operations conditioned by the overload of information systems, by massively accessing certain websites. The result is the cessation, very slow functioning, or even total blocking of networks. This is a popular method both in the civilian and military sectors[26].

Although cyber threats are not unprecedented, says cybersecurity expert Benoît Grunemwald, in the context of the Russo-Ukrainian war, we are witnessing an intensification of cyber attacks from Russia on Ukraine. The war between Russia and Ukraine can be characterized not only as a war fought on the ground through the use of force but also as an active war conducted in cyberspace. There are no planes or tanks here, but computers and the internet are the only weapons. For Michel Baud, "the war in Ukraine, especially in cyberspace, represents a well-coordinated operation carried out by a group of citizens through information and communication systems"[27].

The cyber war, as part of the Russian Federation's military aggression in Ukraine, has been significant, marking the largest conflict in the cyber era. The cyber operations have been extensive, involving phishing, DDoS attacks, and propaganda. Russia has been a key player, engaging in numerous cyber

[26] M. Fürstenau, *Ucrania: tropas convencionales y guerreros virtuales,* <https://www.dw.com/es/guerra-en-ucrania-tropas-convencionales-y-cibercombatientes-invisibles/a-65403959> (12.09.2024).

[27] C. Dugoin-Clément, *Ukraine, crises, conflicts, droit international et cyberspace,* chrome-<extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.defnat.com/pdf/Dugoin-Clement%20(T%201542)_0ML8HxA2l.pdf> (12.09.2024).

operations against Ukraine. Thus, the cyber attacks are part of Russia's strategy to wage an informational war, used alongside conventional military tactics[28]. A number of hackers aligned with the Russian government have carried out hundreds of cyber attacks against Ukraine since Moscow invaded the neighboring country, said the American giant Microsoft in a report. Microsoft emphasized that in Russia's "hybrid" warfare tactics, these cyber attacks are often combined with military actions on the battlefield. "Even before the invasion, we saw at least six national actors aligned with Russia launching over 237 operations against Ukraine," detailed Microsoft, which works with Ukrainian cybersecurity experts and private companies to counter such attacks. The company claimed that this cyber war has included "destructive attacks that are ongoing and threaten civilian welfare." It also stated that it has detected nearly 40 destructive cyber attacks, targeting hundreds of systems, with one-third directly targeting Ukrainian government organizations at all levels (national and local), while another 40% targeted the country's critical infrastructure. "These actors often modify their malware with each action taken to avoid detection," the report mentioned. According to statements presented in the report, cyber attackers began preparing the campaign in March 2021, nearly a year before Vladimir Putin ordered Russian troops to invade Ukraine[29].

According to information published by UATV citing the Security Service of Ukraine, Russia carries out an average of over ten cyber attacks per day on the neighboring country. Throughout the year 2022, the SBU stopped over 4,500 cyber attacks directed towards Ukraine. Furthermore, even before the war between the two states began, Ukraine had repelled numerous massive attacks. As expected, since the beginning of the Russo-Ukrainian war, the number of attacks has significantly increased. To get a comprehensive picture of the situation regarding Russia's cyber attacks on Ukraine, it is necessary to compare the launched attacks. Thus, in 2020, around 800 cyber attacks were launched against Ukraine. By 2021, this number had increased to 1,400, and in 2022, it reached over 4,000 cyber attacks. From this, we see how the Russian Federation resorts to the use of special cyber operations to target energy, logistics, and military installations, as well as the computing centers of Ukrainian state organizations—a significant detail, as it differentiates modern

[28] C. Soare, *Invazia rusă în Ucraina, devine şi primul război cibernetic din istorie: Kievul susține că Rusia se folosește de cooperarea cu China pentru a efectua atacuri cibernetice*, <https://www.defenseromania.ro/invazia-rusa-in-ucraina-in-primul-razboi-cibernetic-din-istorie-kievul-sustine-ca-rusia-se-foloseste-de-cooperarea-cu-china-pentru-a-efectua-atacuri-cibernetice_626906.html#google_vignette> (12.09.2024).

[29] *Guerre en Ukraine: Pourquoi.., op. cit.*

wars from wars of the past. It is about depriving the other party of obtaining resources, in fact. Additionally, it is a wise move to attack databases[30].

Ukraine is often described as a playground for Russian hackers, who have conducted attacks to test techniques and tools. In 2015, Ukraine's power grid was disrupted by a cyber attack called Black Energy, which caused a short-term outage for around 80,000 customers of a utility company in western Ukraine. A year later, another cyber attack known as Industroyer left nearly a fifth of Kiev's population without electricity for about an hour[31].

With the onset of the ground invasion, a wave of cyber attacks on critical infrastructure in Ukraine such as nuclear or electrical power plants, water purification and treatment plants, gas distribution centers, communication antennas and towers, railways, etc., was expected. However, in a scenario of ground war conflict, most of these attacks were carried out through physical bombardments rather than the sophisticated cyber attacks that had been planned. These operations were reported by various Russian media sources, as well as by the creation of specific platforms and accounts on social networks for this purpose[32].

In many cases, third parties were paid for their maintenance and management. Indeed, one of the conclusions that can be drawn from what was observed in the war in Ukraine is that Russia, in addition to military forces, resorts to the use of cyber forces that have not always been its own. In many cases, the Russian government funded cybercriminals and mafias to carry out various operations as mercenaries, leveraging the knowledge they had from their traditional activities before the war. This is the case with various ransomware mafias or botnet owners. There were even groups that supported these campaigns for ideological reasons, without the need for significant economic incentives. These types of attacks usually attempt to collect sensitive information about troop movements, military strategy, supply of essential goods and weapons, etc. In practice, in all cases, there were spear-phishing attacks, meaning illegitimate emails carefully crafted so as not to raise suspicions among their victims and to be perceived as legitimate and trustworthy. When these attacks were successful, the access credentials of the victims were compromised, allowing adversaries to access critical resources, almost always data. This data was not always related to the collection of military information; sometimes, it was used in default campaigns both in Ukraine and in other allied countries. Hack-and-leak operations usually leak

[30] *Así es la guerra cibernética que están librando Rusia y Ucrania. Las trincheras digitales en 2022*, <https://cincodias.elpais.com/cincodias/2022/12/27/lifestyle/1672132222_772838.html#> (12.09.2024).

[31] J. Tidy, *Rusia y Ucrania: los 3 ciberataques rusos que más teme Occidente*, <https://www.bbc.com/mundo/noticias-60850173> (12.09.2024).

[32] *Ibidem*.

information about the victims of Ukrainian combatants, the hesitancy of various governments when it comes to sending weapons to Ukraine, internal discussions about military strategy or peace negotiations, etc. In addition to the aforementioned attacks, others have been observed, which deserve attention due to their novelty or sophistication, almost all related to telecommunications infrastructures. The first was the attack on Viasat an hour before the invasion began. This is an American company in which the Ukrainian army trusted to provide satellite communications links[33].

The Russian military used malware called AcidRain to completely disable thousands of communication terminals in the KA-SAT network, including routers and modems. This attack also affected other European infrastructures, such as wind power generation turbines. The second attack repeated in recent months was based on hijacking Border Gateway Protocol (BGP) sessions. These types of attacks allow the manipulation of routing protocols on which the Internet relies, so that routers can select the worst-intentioned paths for network traffic passing through attacker-controlled devices.

Some experts predicted an escalation in 2023 of cyber attacks carried out by Russia, both in terms of number and scope, as well as potential victims. These attacks have been a powerful tool to reach areas of Ukraine further away from regions subject to traditional warfare, while Russian forces were bogged down in the Eastern part of the country[34]. Pro-Moscow hackers "used destructive programs to disrupt and degrade Ukraine's military and government capabilities," including attacking civilian infrastructure to undermine Ukrainians' confidence in national capabilities[35].

Since the beginning of the war, Russia has implemented at least nine families of Wiper malware and two types of ransomware against over 100 Ukrainian government and private organizations[36]. Strong public-private cyber defense arrangements, as well as Ukrainian preparedness and resilience, have

[33] *Ibidem.*

[34] M. Beltrán, *El papel del ciberconflicto en Ucrania sigue siendo una incógnita un año después,* <https://www.eleconomista.com.mx/tecnologia/El-papel-del-ciberconflicto-en-Ucrania-sigue-siendo-una-incognita-un-anodespues-20230506-0028.html> (12.09.2024).

[35] *Los ciberataques rusos aumentaron un 300% en 2022 en países de la OTAN,* <https://www.france24.com/es/minuto-a-minuto/20230216-los-ciberataques-rusos-aumentaron-un-300-en-2022-en-pa%C3%ADses-de-la-otan> (12.09.2024).

[36] M. G. Pascual, *Por qué Rusia no ha logrado ganar la guerra cibernética en Ucrania*, <https://elpais.com/tecnologia/2023-02-14/por-que-rusia-no-ha-logrado-ganar-la-guerra-cibernetica-en-ucrania.html> (12.09.2024).

successfully defended against most of these attacks, but Russia's activity continues[37].

According to statements made in London by Viktor Zhora, a member of the leadership of the State Special Communications and Information Protection Service of Ukraine, "cyber attacks on Ukraine's infrastructure have tripled during the war months and have often been destructive"[38]. The impact of cyber attacks on Ukraine from Russian actors is presented in the report of the Ukrainian SSSCIP service. Thus, according to the report, there is evidence demonstrating that Russia is waging a war that fits the pattern of hybrid warfare. SSSCIP gives the example of Russian attacks on the energy sector, which are said to have been a significant target of Russian hackers since the beginning of the invasion. Furthermore, the report shows that cyber attacks and those on the media sector usually precede conventional attacks. The SSSCIP study shows that Russia's conventional attacks are often preceded by cyber attacks, which is why the war in Ukraine also falls within the parameters of cyber warfare. Although Russia has repeatedly denied that hacker attacks are orchestrated by the Kremlin, according to SSSCIP, cyber attacks on Ukraine have tripled since the beginning of the war.

In this context, attention should also be paid to the analysis elaborated by specialists from Check Point Research, according to which, cyber attacks in the first days of the Russian invasion and the number of cyber attacks on Ukrainian government infrastructure increased by 196%, while attacks on the Ukrainian commercial sector increased by 4%. Furthermore, according to research conducted by experts from Check Point Research, cyber attacks against Ukraine began in 2014, following the illegal annexation of Crimea, intensifying from February 2022 onwards, affecting the distribution chains of medicines, food, and war supplies most severely[39].

The attacks have taken various forms, but among the tactics used most frequently are deepfakes, phishing emails, malware attacks, Distributed Denial of Service (DDoS) attacks, and information theft. According to SSSCIP, cyber attacks on Ukraine have tripled since the beginning of the war. However, cyber warfare traces its roots back to 2014, the year of Russia's annexation of Crimea. In March 2014, when Russia began its strategy to annex the territory, a DDoS attack hit Crimea's communication systems. Although cyber attacks often precede conventional attacks, sometimes they occur in tandem. One month

[37] *¿Se está reagrupando Rusia para una nueva ciberguerra*?, https://news.microsoft.com/es-es/2023/03/17/se-esta-reagrupando-rusia-para-una-nueva-ciberguerra/> (12.09.2024).

[38] D. Temple-Raston, *In recent interview, ousted Ukrainian cyber official spoke about new Russian attacks, long-term plans*, <https://therecord.media/victor-zhora-interview-click-here-ousted> (12.09.2024).

[39] *2023 Cyber Security Report*, <ttps://www.mvrop.org/cms/lib/CA01922720/Centricity/Domain/59/2023-cyber-security-report.pdf> (12.09.2024).

before the invasion of Ukraine, hackers displayed the message "expect the worst" on 70 official government websites[40]. In May 2022, DDoS attacks continue against Ukraine. They target the city council of Odessa, a cyber attack followed by a conventional one on the residential infrastructure of the city. Thus, Russia's strategy is to show doubt among the Ukrainian population about the government's ability to manage the country's infrastructure. SSSCIP states that "cyber attacks are designed to escalate the chaos of conventional invasion, to disrupt the administration of the country, and to cause major damage to infrastructure"[41].

According to the State Special Communications and Information Protection Service of Ukraine, cyber aggression is an offensive tactic of Russia. This takes the form of cyber attacks on communication services and institutions of the country[42]. In this context, several Ukrainian state agencies, including the state energy company, reported cyber attacks or technical disruptions on January 24, 2024, affecting their IT systems and their ability to communicate with the public. Naftogaz, Ukraine's largest oil and gas company, stated that a "large-scale cyber attack" on one of its data centers took its website and call centers offline. Additionally, within the context of cyber attacks conducted by the Russian Federation against Ukraine, there is also the piracy on January 21, 2024, targeting a Ukrainian bank: The largest mobile-only bank in Ukraine was targeted by hackers. Thus, Monobank was targeted with 580 million service requests in a single attack. It is worth noting the cyber attacks against Ukrainians on the eve of the NATO Summit on July 11-12 in Vilnius, Lithuania. BlackBerry researchers have determined that the threat actor was RomCom, who targeted Ukraine supporters scheduled to attend the conference[43].

In this context, Microsoft has issued warnings about a credential theft campaign backed by Russia. Microsoft's security team stated that evidence of cyber attacks orchestrated by the state-backed group Midnight Blizzard, also known as Nobelium, has been found, targeting personal credentials. Midnight Blizzard hackers use residential proxy services to obfuscate the source IP address of their attacks, which typically target governments, IT service providers, NGOs, the defense industry, and critical manufacturing. Additionally, Nobelium is believed to be behind attacks on Ukrainian military

[40] I. Breilean, *Războiul cibernetic. Istoria atacurilor rusești și mărturia unui voluntar din „Armata IT" a Ucrainei*, <https://romania.europalibera.org/a/razboi-cibernetic-aramata-it-ucraina/32235520.html> (12.09.2024).

[41] *Ibidem.*

[42] *Ibidem.*

[43] J. Masters, *Russia-Ukraine War: Cyberattack – Kinetic Warfare Timeline*, <https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion> (12.09.2024).

targets, countries providing military assistance to Ukraine, and other organizations opposing Russia[44].

A wave of cyber attacks targeting Ukrainian government agencies and information technology vendors occurred on June 15, 2023, by a group called "Cadet Blizzard," which has been active since 2020. Furthermore, in the context of analyzing Russia's cyber attacks on Ukraine, the activity of the 16th Unit (known as Turla, an elite Russian espionage group) of the Russian Federal Security Service, or FSB, is noteworthy. They used versions of the Snake malware program to create a peer-to-peer network of hundreds of infected computers to remove material belonging to US allies in North America. The pro-Russian hacktivist group Killnet, a cyber crew posing as "hacktivists" actively targeting opponents of the Russian invasion of Ukraine, is also notable. The responsible for widespread denial of service (DDoS) attacks in Europe and the US, at the end of April, they reorganize as a "private military hacking company." Similarly, Russia's activity in launching malware campaigns against Ukraine includes the Iridium campaign (alias Sandworm). It is believed that Iridium is associated with Russia's military intelligence agency (GRU) and prepares operations in a similar manner to the deployment of malware Foxblade and Caddywiper in the early days of the war[45].

Analyzing the cyber attacks carried out by Russia, they can be divided into three categories[46]:

1. Trust Attacks. Trust attacks refer to cyber attacks that undermine public trust in the government's ability to protect its citizens and provide essential services. In the first week of March 2022, it is believed that some Russian cyber actors were involve in launching DDoS attacks (cyber attacks where website servers are flooded with traffic until they become unstable) against the website of the Ministry of Defense of Ukraine. Similarly, the Russian cyber actor FancyBear was found responsible for engaging in a phishing campaign against a Ukrainian media company, UkrNet.
2. Capability-based Attacks. The capability-based attacks are cyber attacks where the adversary's power is undermined by exploiting cyber weapons to gain access to the adversary's critical infrastructure and disrupt its capabilities. In this context, actions taken by several attackers, believed to be of Russian nationality, during the invasion of

[44] *Ibidem*.

[45] J. Masters, *Russia-Ukraine War: Cyberattack – Kinetic Warfare Timeline*, <https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion> (12.09.2024)

[46] *Dimensiunea cibernetică a conflictului Rusia – Ucraina - Deslușirea primei etape*, <https://dnsc.ro/citeste/dimensiunea-cibernetica-conflictului-rusia-ucraina-deslusirea-primei-etape> (12.09.2024).

Ukraine on February 24, 2022, by Russia, serve as examples. As a result, these actions resulted in the destruction of tens of thousands of satellite internet modems in Ukraine and Eastern Europe. These actions are considered to be among the largest cyber attacks in a war, causing massive disruption to communications at the onset of the conflict. In the initial phase of the war, the prominent Russian cyber actor Sandworm was largely absent for unknown reasons. However, the group made its presence felt in the second phase when it was revealed that they attempted to cause a power outage through malware that could have affected two million people.

3. Control-based Attacks. The control-based attacks refer to physical attacks on cyber infrastructures, where the main goal is to gain control over the adversary's critical infrastructure. From this perspective, two notable cyber attacks stand out: 1) on March 1, 2022, a projectile strike on television towers in Kiev coincided with a cyber attack on media companies, and 2) a few days later, during the occupation of the Europe-Zaporizhzhia nuclear power plant, a Russian cyber actor was detected in the networks of a Ukrainian nuclear energy company.

The attackers supported by the Russian government have engaged in an aggressive effort on multiple fronts to gain a decisive advantage in the cyber warfare space, often with mixed results. This includes a significant shift in the focus of various groups towards Ukraine, a dramatic increase in the use of destructive attacks against the Ukrainian government, military and civilian infrastructure, a rise in spear-phishing activity targeting NATO countries, and an increase in cyber operations. For example, it has been observed that threat actors breach sensitive information to promote a specific narrative. Russian government-supported attackers intensified cyber operations starting in 2021, in the lead-up to the invasion. In 2022, Russia increased targeting of users in Ukraine by 250% compared to 2020. In 2022, attackers supported by the Russian government targeted users in Ukraine more than any other country. While we see these attackers heavily focused on the Ukrainian government and military entities, the campaigns we have disrupted also show a strong emphasis on critical infrastructure, utilities, and public services, as well as media and informational space. Many operations have indicated an attempt by the Main Directorate of the General Staff of the Russian Armed Forces (GRU) to balance competing priorities of access, collection, and disruption throughout each stage of activity.

During this period, the public, energy, media, financial, business, and non-profit sectors in Ukraine suffered the most. Starting from February 24, 2022, Russia's cyber attacks on Ukraine undermined the distribution of medicines, food, and aid. Their impact ranged from hindering access to basic services to data theft and disinformation, including through deepfake technology. Other malicious cyber activities involve phishing emails, distributed denial-of-service attacks, and the use of data-wiping malware, backdoors, surveillance software, and information stealers. The organizations and governments worldwide have not been indifferent to the hybrid risks presented. Initiatives led by the EU, US, and NATO have been undertaken to neutralize cyber threats and protect critical infrastructure. As part of these initiatives, the EU has activated its cyber rapid response teams (a project under the Permanent Structured Cooperation (PESCO) in the field of security and defense policy) to support Ukraine's cyber defense. Non-governmental and private actors have supported Ukraine through various cyber resilience activities. Since the beginning of the invasion, a significant number of counterattacks have been launched by independent hackers, affecting state, security, banking, and media systems in Russia. The European Parliament has called for intensified cyber security assistance to Ukraine and for the full use of the EU's cyber sanctions regimes against individuals, entities, and bodies responsible for or involved in various cyber attacks targeting Ukraine[47].

The Ukraine-and West cooperation in combating cyber threats

Russia has created the greatest threat to peace and stability in Europe since World War II. Since 2014, the driving force behind the development of the Ukrainian cyber space has been the war with Russia. Although authorities have not been able to act effectively in the cyber space since the beginning of the conflict, it has given rise to a cyber ecosystem capable of adapting to the wartime context. This ecosystem has contributed to the defense of the country at all levels, both among citizens and among state and private actors. Although there are still many objectives to be achieved, the invasion of Ukraine has become a catalyst for cyber development, which has become a key player in the Department of Defense. In addition to kinetic warfare, Ukraine currently faces the enemy in both its informational space and in the cyber domain, areas that have often been considered secondary in a high-intensity armed conflict. Cyber sabotage, as well as cyber espionage, are integral parts of the conflict. Taken by surprise by the absence of national cyber security and a clear policy on pollution of the infosphere, Ukrainian authorities have been led to make colossal efforts in the cyber domain[48].

[47] *Russia's war on Ukraine: Timeline of cyber-attacks*, <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549> (12.09.2024).

[48] A. Kryvetska, *Comment l'écosystème cyber ukrainien s'est-il adapté à la guerre?*, <https://www.diploweb.com/Comment-l-ecosysteme-cyber-ukrainien-s-est-il-adapte-a-la-guerre.html> (20.09.2024).

According to statements by Josep Borrell, the High Representative for Foreign Affairs and Security Policy, the Council has made decisions regarding a series of measures to support Ukraine's resilience against Russian aggression. The Council has adopted a decision to provide macro-financial assistance of 1.2 billion euros and has decided to support the professional military training of Ukraine under the European Peace Instrument. Additionally, the EU will enhance its support for combating cyber attacks and disinformation by sending a mission of experts to the country[49].

In order to counter Russian cyber attacks, Ukraine has signed security agreements with its Western allies, hoping to receive additional support in cyber security, military, and humanitarian areas as the ongoing war with Russia reaches the three-year mark. Security agreements for Ukraine are based on the commitment made by the Group of Seven (G7) countries in July 2023. Ukraine has already concluded 10-year agreements with the United Kingdom, Germany, France, and Denmark – the first non-G7 country to finalize the agreement. Additionally, Norway, the Netherlands, and Italy have offered their support to Ukraine for strengthening the defense industry and countering hybrid threats, such as cyber warfare[50].

According to the agreements, Ukraine will receive support in five areas where the war is being waged - on land, in the air, at sea, in space, and in the cyber domain. The cyber support primarily involves assistance to help Ukraine protect its networks from Russian cyber attacks and counter disinformation. For example, the security agreement with Denmark, signed during Danish Prime Minister Mette Frederiksen's visit to Ukraine, promises to assist Ukraine in "preventing, detecting, and countering Russian cyber aggression, cyber espionage, and hybrid warfare". This also includes "strengthening cyber diplomacy, providing technical assistance to Ukraine, and enhancing its cyber resilience". Germany has also committed to helping Ukraine protect its infrastructure from cyber attacks and to modernize the country's security and information architecture, according to the agreement concluded in early February. Berlin will also provide training for Ukrainian experts in cyber security "based on EU standards in IT security".

In this context, the support offered to Ukraine by France is also noteworthy. France will collaborate with Ukraine "to increase the cost of irresponsible use of cyber capabilities by Russia and other hostile state and non-state actors". Paris will also assist Kyiv in combating cybercrime and organized crime[51].

[49] *Consiliul Afaceri Externe, 21 februarie 2022*, <https://www.consilium.europa.eu/ro/meetings/fac/2022/02/21/> (20.09.2024).

[50] *Ukraine signs security deals with Western allies to help counter Russian cyberattacks*, <https://therecord.media/ukraine-signs-security-deals-with-western-allies-over-russian-cyberattacks> (20.09.2024).

[51] *Ibidem*.

As the conflict in Ukraine continues, experts have drawn attention to the types of cyber attacks that Russia could conduct against its neighboring country, and thus the international community has mobilized to help the Ukrainian state remotely[52].

As a result of the Joint Declaration of Support for Ukraine jointly issued by the leaders of the Group of Seven (G7) and Ukraine on the margins of the NATO Summit in Vilnius on July 12, 2023 ("G7 Joint Declaration"), the Agreement between Ukraine and Canada was signed on February 24, 2024[53].

Since the large-scale invasion of Ukraine by Russia in February 2022, Canada has provided multidimensional support to Ukraine, including diplomatic, financial, humanitarian, and military assistance, support for development, information, and cyber security, as well as assistance for restoring peace and stability and implementing immigration measures to help Ukrainians settle safely from Russian aggression. Since 2022 and since the beginning of Russia's large-scale invasion of Ukraine, Canada has committed to providing Ukraine with military assistance worth over $2.4 billion. The participants will continue to strengthen their cooperation in defense, building on the strong relationships established between their military and defense institutions since the launch of Operation UNIFIER in 2015, as well as the significant military training and assistance provided by Canada before and after Russia's large-scale invasion.

According to the provisions of Part IV, "Areas of Continued and Enhanced Cooperation and Long-Term Support", Section D, "Cyber Security and Resilience":

1. The states will work together to enable Ukraine to detect, deter, and disrupt Russian cyber aggressions, cyber espionage, and hybrid warfare operations, including maintaining cyber resilience and protecting critical infrastructure against malicious cyber attacks. This objective can be achieved through cooperation and information exchange on cyber threats; implementing joint initiatives; training specialists from defense services, intelligence services, special services, and law enforcement agencies in Ukraine; as well as providing cyber assistance to Ukraine;
2. The participants will work together to detect and deter the irresponsible and malicious use of cyber capabilities by the Russian Federation and other hostile actors, whether state or non-state, against the Participants;

[52] *Acord România-Ucraina privind cooperarea în domeniile digitalizării și protecției cibernetice,* <https://www.euractiv.ro/infosociety/acord-romania-ucraina-privind-cooperarea-in-domeniile-digitalizarii-si-protectiei-cibernetice-65107> (20.09.2024).

[53] *Accord de coopération en matière de sécurité entre le Canada et L'Ukraine*, <https://www.international.gc.ca/world-monde/Issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/agreement-ukraine-accord.aspx?lang=fra> (20.09.2024).

3. Recognizing the importance of building strong cyber defense capabilities against state and non-state actors and wishing to expand cooperation in this important area, the participants will:
   - exchange information on national cybersecurity policies, best practices, and lessons learned to strengthen their respective cyber security and resilience;
   - explore new areas of cooperation and new opportunities in the defense and cybersecurity fields;
   - continue to promote exchanges of experts in this field.

Specifically, Canada will continue to:

- provide specific assistance to Ukraine in the field of cyber defense;
- collaborate with partners to coordinate the strengthening of civilian cyber capabilities in Ukraine. This coordination aims to help Ukraine defend against ongoing malicious cyber activities and meet its long-term cyber resilience needs[54].

An important diplomatic step for Ukraine is the signing of a bilateral security agreement by Emmanuel Macron and Volodymyr Zelensky in Paris on February 16, 2024, guaranteeing long-term civil and military support for Ukraine, which has been at war for two years. This ten-year pact follows the commitments made by the G7 at the NATO Summit in Vilnius in July 2023. In addition to the €1.7 billion in 2022 and €2.1 billion in 2023 provided to Ukraine, France commits to providing €3 billion in additional military support to Ukraine in 2024. Paris aims to help Ukraine strengthen its military capabilities to defend its territory and deter future attacks, providing it with equipment and training for Ukrainian forces. As Russia conducts massive disinformation campaigns, signatories to the agreement commit to "combat digital interference and information manipulation" by Moscow, as well as "global propaganda". The agreement provides for "joint education and training programs" for professionals in information integrity[55].

Thus, according to Chapter II, "Cooperation in Security", Section "General Cooperation to Enhance Ukraine's Security", the partnership with France will help Ukraine join collective tools to combat foreign interference and information manipulation, primarily Russian propaganda and disinformation campaigns. Additionally, according to the agreement provisions, states will collaborate to enable Ukraine to detect, deter, and disrupt cyber aggression,

[54] *Ibidem*.

[55] *Guerre en Ukraine: aide militaire, assistance en cas d'agression... Ce que contient l'accord de sécurité signé entre Kiev et Paris*, <https://www.francetvinfo.fr/monde/europe/manifestations-en-ukraine/guerre-en-ukraine-aide-militaire-assistance-en-cas-d-agression-ce-que-contient-l-accord-de-securite-signe-entre-kiev-et-paris_6371677.html> (20.09.2024).

cyber espionage, including by enhancing cyber resilience and protecting critical infrastructure against cyber attacks, while also supporting Ukraine's modernization and reform of its security architecture and providing international technical services. The participants will work together to increase the cost of the irresponsible use of cyber capabilities by the Russian Federation and other hostile state and non-state actors against the participants. They will also enhance their operational cooperation in fighting cybercrime and deepen Ukraine's cooperation with EU and NATO structures in cybersecurity[56].

The cyber attacks have increased by 300% between 2020 and 2022 in NATO countries, and by 250% in Ukraine, according to a report by Mandiant, a Google-owned specialized company. Ukraine needs support to "detect, deter, and disrupt any cyber aggression, any cyber espionage". Cooperation in information, counterespionage, fighting serious crime, and organized crime is also planned. This involves combating the infiltration of individuals and groups with criminal influence into Ukrainian society. Signatory countries must cooperate in investigations and joint operations[57].

Equally noteworthy is the signing of the agreement for the development of relations in the field of digitization and cyber security by the Romanian Minister of Research, Innovation, and Digitalization, Bogdan Ivan, and the Ukrainian Deputy Prime Minister for Innovation, Development of Education, Science, and Technology, Mykhailo Fedorov. "Through the signed Agreement, Romania strengthens its position as a regional hub for emerging technologies and cybersecurity. Thus, by signing this agreement, the groundwork is laid for a mechanism through which the European Union will finance concrete technology transfer and knowledge projects to Ukraine, projects in which Romania will lead the partnership"[58]. Additionally, the agreement ensures "the basis for close and concrete collaboration" of institutions with responsibilities regarding IT&C infrastructure, digitization, and cyber security in the two countries.

The main areas of action include:

- increasing the resilience and protection of digital infrastructure in Ukraine and Romania;
- strengthening the level of cyber protection of national networks and infrastructures in Ukraine and Romania;

[56] *Accord de coopération en matière de sécurité entre la France et l'Ukraine*, <https://www.elysee.fr/emmanuel-macron/2024/02/16/accord-de-cooperation-en-matiere-de-securite-entre-la-france-et-lukraine> (20.09.2024).

[57] *Guerre en Ukraine: aide militaire.., op. cit.*

[58] S. Cojocaru, *Acord de cooperare româno-ucrainean în domeniul digitalizării şi securităţii cibernetice. Proiectele beneficiază de finanţare UE*, <https://tvrmoldova.md/article/3f68dd806fe63aea/acord-de-cooperare-romano-ucrainean-in-domeniul-digitalizarii-si-securitatii-cibernetice-proiectele-beneficiaza-de-finantare-ue.html> (20.09.2024).

- developing cloud infrastructure for electronic public services;
- exchanging experience in policy formation in the field of electronic communications and emerging technologies[59].

In response to the Russian threat, both private and governmental entities have made unprecedented efforts to support Ukraine's cyber resilience. According to the British publication The Guardian, for the first time since its establishment, the European Union's rapid cyber response team, led by Lithuania, capable of detecting and responding to a variety of threats, has been involved in helping defend Ukraine against cyber attacks. The British publication also mentioned the collaboration between the Romanian state and the private sector to assist the ongoing fight against cyber attacks in the country, specifically the partnership between the National Cyber Security Directorate (DNSC) and Bitdefender, which offered to provide free support and information about potential threats to the Ukrainian state. Additionally, NATO, which has been working with Ukraine for several years to enhance its cyber defense, signed an agreement a few weeks before the invasion aimed at strengthening cyber cooperation with Ukraine. At the same time, in Ukraine, a whole "IT army" of volunteers was gathered in response to the government's request to support cyber defense efforts[60].

The phenomenon we observe today in Ukraine with the creation of a voluntary cyber army ("IT-Army of Ukraine") does not date back to the invasion on February 24, 2022. The genesis of this type of cyber group dates back to the time of the war in Donbass. What do we understand by a "cyber volunteer”? This is an individual who voluntarily participates in defending his country through cyberspace without financial compensation. It can be either an "ordinary" citizen or an experienced hacker. Generally, two categories are observed: autonomous formations that bring together people of all levels on one hand, and on the other hand, groups of hackers responsible for carrying out sophisticated cyber attacks on enemy infrastructure[61].

Conclusions

With the increasing dependency of society on technology and the internet, new forms of threats to the security of not only states but also businesses and individuals worldwide have emerged - cyber attacks, known as cyber warfare.

[59] *Accord România-Ucraina..., op. cit.*

[60] G.-A. Cristescu, *Mobilizare pentru apărarea cibernetică a Ucrainei. România, în atenţia presei internaţionale după anunţul autorităţilor de a colabora* cu Bitdefender, <https://adevarul.ro/stiri-interne/evenimente/mobilizare-pentru-apararea-cibernetica-a-ucrainei-2154479.html> (20.09.2024).

[61] A. Kryvetska, *op. cit.*

The cyber warfare has become a real threat today, and advanced technology is now a powerful tool to attack, sabotage, and disable the information systems of a country. Due to its transnational and anonymous nature, cyber warfare presents unique challenges to the security of states compared to other forms of conflict. Although the boundaries of cyber warfare may be unclear, as in conventional warfare, the primary objective of cyber warfare is to weaken a country by undermining social cohesion, political stability, and the military and industrial capacity of a state.

The cyber warfare is a growing form of conflict that can have serious consequences for society.

Thus, analyzing the cyberattacks carried out by the Russian Federation against Ukraine, Moscow resorts to leveraging the entire spectrum of IO - from state-sponsored mass media to hidden platforms and accounts. It is worth mentioning that they have been present in the cyber space for over a decade, examining the types of attacks that Russian cyber actors launch in Ukraine, since the Russian cyberattacks against Estonia. The military tensions between Russia and Ukraine have clashed in a continuous cyber conflict for about ten years. Kremlin-backed hackers have unleashed the most destructive cyberattacks in history in recent years. However, the danger of escalating conflict in the cyber domain should not be underestimated, as there are no geographical limits to Russian attack attempts.

In the current circumstances, as the Russian Federation decides to the use of cyber attacks as weapons and tactics to pursue its own interests, it is important for the international organizations, governments, businesses, and individuals to strengthen collaboration to mitigate and diminish risks and to protect their own information systems, including safeguarding their own security. Furthermore, the use of cyber attacks by Russia necessitates urgent measures by the world's states to mitigate the impact that cyber attacks can have on national security, as well as international security. Currently, ensuring cyber security must be viewed as an imperative of the time and a critical priority for national defense and the protection of society as a whole.

BIBLIOGRAPHY:

1. *Accord de coopération en matière de sécurité entre le Canada et L'Ukraine*, <https://www.international.gc.ca/world-monde/issues_ development-enjeux_developpement/response_conflict-reponse_ conflits/crisis-crises/agreement-ukraine-accord.aspx?lang=fra>
2. *Accord de coopération en matière de sécurité entre la France et l'Ukraine*,

<https://www.elysee.fr/emmanuel-macron/2024/02/16/ accord-de-cooperation-en-matiere-de-securite-entre-la-france-et-lukraine>

3. *Acord România-Ucraina privind cooperarea în domeniile digitalizării și protecției cibernetice,* <https://www.euractiv.ro/infosociety/acord-romania-ucraina-privind-cooperarea-in-domeniile-digitalizarii-si-protectiei-cibernetice-65107>
4. Arman D., *Atacul cibernetic-o nouă formă de agresiune în dreptul internațional,* <https://ibn.idsi.md/sites/default/files/imag_file/28-31_23.pdf>
5. *Así es la guerra cibernética que están librando Rusia y Ucrania. Las trincheras digitales en 2022,* <https://cincodias.elpais.com/cincodias/ 2022/12/27/lifestyle/1672132222_772838.html#>
6. Balmforth T., *Exclusive: Russian hackers were inside Ukraine telecoms giant for months,* <https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/>
7. Beltrán M., *El papel del ciberconflicto en Ucrania sigue siendo una incógnita un año después,* <https://www.eleconomista.com.mx/tecnologia/El-papel-del-ciberconflicto -en-Ucrania-sigue-siendo-una-incognita-un-anodespues-20230506-0028.html>
8. Blanc-Rolin C., *Conflit Russie-Ukraine: la guerre est aussi cyber,* <https://www.dsih.fr/article/4608/conflit-russie-ukraine-la-guerre-est-aussi-cyber.html>
9. Breilean I., *Războiul cibernetic. Istoria atacurilor rusești și mărturia unui voluntar din „Armata IT” a Ucrainei,* <https://romania.europalibera.org/a/razboi-cibernetic-aramata-it-ucraina/32235520.html>
10. Buxton O., *Ciberguerra: tipos, ejemplos y cómo protegerse,* <https://www.avast.com/es-es/c-cyber-warfare>
11. Cojocaru S., *Acord de cooperare româno-ucrainean în domeniul digitalizării şi securităţii cibernetice. Proiectele beneficiază de finanţare UE,* <https://tvrmoldova.md/article/3f68dd806fe63aea/acord-de-cooperare-romano-ucrainean-in-domeniul-digitalizarii-si-securitatii-cibernetice-proiectele-beneficiaza-de-finantare-ue.html>
12. Consiliul Afaceri Externe, 21 februarie 2022, <https://www.consilium.europa.eu/ro/meetings/fac/2022/02/21/>
13. *Cyber warfare: ¿Qué es la guerra cibernética?,* <https://www.metacompliance.com/es/cyber-security-terminology/ cyber-warfare>
14. De Santos J. C., *Ucrania | La realidad ha dejado a la guerra cibernética en un segundo plano,* <https://es.euronews.com/2023/02/22/

ucrania-la-realidad-ha-dejado-a-la-guerra-cibernetica-en-un-segundo-plano>

15. *Dimensiunea cibernetică a conflictului Rusia – Ucraina - Deslușirea primei etape,* <https://dnsc.ro/citeste/dimensiunea-cibernetica-conflictului-rusia-ucraina-deslusirea-primei-etape>
16. Dugoin-Clément C., *Ukraine, crises, conflicts, droit international et cyberespace*, <https://www.defnat.com/pdf/Dugoin-Clement%20(T%201542)_0ML8HxA2l.pdf>
17. Fürstenau M., *Ucrania: tropas convencionales y guerreros virtuales*, <https://www.dw.com/es/guerra-en-ucrania-tropas-convencionales-y-cibercombatientes-invisibles/a-65403959>
18. Gavrila A., *La gran ciberguerra de Ucrania que no ocurrió*, <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO99_2022_ADAGAV_Ucrania.pdf>
19. Guedes R., *Guerra Cibernética: Tipos, Armas, Objetivos y Ejemplos de Guerra Tecnológica*, <https://ciberprisma.org/2023/05/10/guerra-cibernetica-tipos-armas-objetivos-y-ejemplos-de-guerra-tecnologica/>
20. *Guerre en Ukraine: aide militaire, assistance en cas d'agression ... Ce que contient l'accord de sécurité signé entre Kiev et Paris*, <https://www.francetvinfo.fr/monde/europe/manifestations-en-ukraine/guerre-en-ukraine-aide-militaire-assistance-en-cas-d-agression-ce-que-contient-l-accord-de-securite-signe-entre-kiev-et-paris_6371677.html>
21. *Guerre en Ukraine: Pourquoi parle-t-on d'une cyberguerre?*, <https://guardia.school/le-lab/guerre-en-ukraine-pourquoi-parle-t-on-dune-cyberguerre.html>
22. *Guerre Russie/Ukraine, une cyber guerre déclarée ?*, <https://tehtris.com/fr/blog/guerre-ukraine-russie-une-cyber-guerre-declaree/>
23. Kryvetska A., *Comment l'écosystème cyber ukrainien s'est-il adapté à la guerre?*, <https://www.diploweb.com/Comment-l-ecosysteme-cyber-ukrainien-s-est-il-adapte-a-la-guerre.html>
24. Libicki M. C., *Cyberwar as a Confidence Game*, <https://www.jstor.org/stable/26270514?seq=8>
25. *Los ciberataques rusos aumentaron un 300% en 2022 en países de la OTAN*, <https://www.france24.com/es/minuto-a-minuto/20230216-los-ciberataques-rusos-aumentaron-un-300-en-2022-en-pa%C3%ADses-de-la-otan>
26. Mackay J., *Cyber warfare: ¿Qué es la guerra cibernética?*, <https://www.metacompliance.com/es/blog/security-awareness-training/what-is-cyber-warfare>
27. Masters J., *Russia-Ukraine War: Cyberattack – Kinetic Warfare Timeline*,

<https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion>

28. Pascual M. G., *Por qué Rusia no ha logrado ganar la guerra cibernética en Ucrania*, <https://elpais.com/tecnologia/2023-02-14/por-que-rusia-no-ha-logrado-ganar-la-guerra-cibernetica-en-ucrania.html>
29. *¿Qué es un ataque cibernético?*, <https://www.ibm.com/mx-es/topics/cyber-attack>
30. *Rusia coordina ciberataques en Ucrania, según Microsoft*, <https://www.dw.com/es/rusia-coordina-ataques-cibern%C3%A9ticos-y-militares-en-ucrania-seg%C3%BAn-microsoft/a-61615216>
31. *Russia's war on Ukraine: Timeline of cyber-attacks,* <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)73354>
32. *¿Se está reagrupando Rusia para una nueva ciberguerra?*, <https://news.microsoft.com/es-es/2023/03/17/se-esta-reagrupando-rusia-para-una-nueva-ciberguerra/>
33. Soare C., *Invazia rusă în Ucraina, devine şi primul război cibernetic din istorie: Kievul susține că Rusia se folosește de cooperarea cu China pentru a efectua atacuri cibernetice*, <https://www.defenseromania.ro/invazia-rusa-in-ucraina-in-primul-razboi-cibernetic-din-istorie-kievul-sustine-ca-rusia-se-foloseste-de-cooperarea-cu-china-pentru-a-efectua-atacuri-cibernetice_626906.html#google_vignette>
34. Temple-Raston D., *In recent interview, ousted Ukrainian cyber official spoke about new Russian attacks, long-term plans,* <https://therecord.media/victor-zhora-interview-click-here-ousted>
35. Tidy J., *Rusia y Ucrania: los 3 ciberataques rusos que más teme Occidente*, <https://www.bbc.com/mundo/noticias-60850173>
36. Trifunović D., Bjelica Z., *Cyber war – trends and technologies*, <https://www.researchgate.net/publication/349942064_Cyber_War_-_Trends_and_Technologies>
37. *2023 Cyber Security Report*, <https://www.mvrop.org/cms/lib/CA01922720/Centricity/Domain/59/2023-cyber-security-report.pdf>
38. *Ukraine signs security deals with Western allies to help counter Russian cyberattacks*, <https://therecord.media/ukraine-signs-security-deals-with-western-allies-over-russian-cyberattacks>
39. <https://www.cisco.com/c/dam/global/es_mx/products/pdfs/58-60-bridge.pdf>
40. *5 amenințări asupra securității cibernetice a statelor europene în contextul războiului ruso-ucrainean*, <https://bit-sentinel.com/ro/5-amenintari-asupra-securitatii-cibernetice-a-statelor-europene-in-contextul-razboiului-ruso-ucrainean/>